Service Organization Control (SOC) 1

Compliance Process

esm_logo.jpg

Nexelus USA  
New York, NEW YORK (NY)  
646-558-1950 ext.128

**9/28/2021**

Contents

[What is SOC 2 Compliance 1](#_Toc83734528)

[SOC 2 compliance Requirements 2](#_Toc83734529)

[Other SOC 2 Compliance Requirements 4](#_Toc83734530)

[1. Availability 4](#_Toc83734531)

[Deliverables 4](#_Toc83734532)

[2. Processing integrity 4](#_Toc83734533)

[Deliverables 5](#_Toc83734534)

[3. Confidentiality 5](#_Toc83734535)

[Deliverables 5](#_Toc83734536)

[4. Privacy 5](#_Toc83734537)

[Privacy Principles 5](#_Toc83734538)

[Information Categories Covered in Privacy Protections 6](#_Toc83734539)

[Deliverables 7](#_Toc83734540)

# What is SOC 1 Compliance

Service Organization Control (SOC) 2 is a set of compliance requirements and research procedures aimed at third-party service providers. It is designed to help companies determine if their business partners and vendors can safely manage data and protect the interests and privacy of their customers.

SOC 2 was developed by the American Institute of Certified Public Accountants (AICPA). Within its processes, there are two types of SOC 2 reports:

**SOC 2 Type 1** details about the systems and controls you have for security compliance. Auditors check the evidence and verify that you are meeting the appropriate standards of trust. Think of it as a time point confirmation of controls.

**SOC 2 Type 2** evaluates how your processes work in providing the desired level of security and data management over a period of time.



## Reference Material:

Content in this document has been compiled using information from following sources:

1. <https://www.venminder.com/blog/6-tips-understanding-a-soc-1-report>
2. <https://en.wikipedia.org/wiki/ITGC>
3. <https://kirkpatrickprice.com/white-papers/soc-1-compliance-checklist-are-you-prepared-for-a-soc-1-audit/>

# SOC 2 compliance Requirements

One of the first key areas to review on SOC reports is the scope. Which services, locations and control areas were included within the SOC report can be found within the service auditor’s report, that is in section two of report. Make sure that the service you use is listed here. Many vendors have multiple SOC reports for different products, and services, and you wouldn’t be the first to be given the wrong one.

In the following paragraphs within the Scope section, look for language such as “The description includes only the control objectives…” and “…excludes the control objectives…” as these typically signify what, if any, aspect of the service is carved out due to the use of a critical subservice organization. A subservice - or third party to the vendor, your fourth party – is an organization that if it were to cease to operate, services offered by the vendor would be affected. This is very commonly seen with a data center or cloud service provider.

## What is excluded from the SOC 1 Report?

Subservice organizations are often used by vendors to provide a part of their service. Some subservice organizations will be critical to your vendors and they should be monitored. Within the auditor’s report section near the sentences noted in the prior section, the report should also outline what services the subservice provides on behalf of the vendor.

If there’s a subservice organization involved, know that it could be a separate vendor or it could be another division or business unit, also known as an internal subservice organization. The most common internal subservice is information technology resulting in an **Information Technology General Controls** (ITGC) report that you’ll also want to review in this instance. Reviewing the ITGC helps verify the integrity of the data security and processes in place.

# General Computer Controls

TGCs may also be referred to as General Computer Controls (GCC) which are defined as: Controls, other than application controls, which relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications, the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.

## Global Technology Audit Guide (GTAG)

GTAGs are written in straightforward business language to address a timely issue related to information technology (IT) management, control, and security. To date, the Institute of Internal Auditors (IIA) has released GTAGs on the following topics:

GTAG 1: Information Technology Controls

GTAG 2: Change and Patch Management Controls: Critical for Organizational Success

GTAG 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment

GTAG 4: Management of IT Auditing

GTAG 5: Managing and Auditing Privacy Risks

GTAG 6: Managing and Auditing IT Vulnerabilities

GTAG 7: Information Technology Outsourcing

GTAG 8: Auditing Application Controls

GTAG 9: Identity and Access Management

GTAG 10: Business Continuity Management

GTAG 11: Developing the IT Audit Plan

GTAG 12: Auditing IT Projects

GTAG 13: Fraud Prevention and Detection in the Automated World

GTAG 14: Auditing User-developed Applications

GTAG 15: Formerly Information Security Governance--Removed and combined with GTAG 17

GTAG 16: Data Analysis Technologies

GTAG 17: Auditing IT Governance

## Complementary User Entity Controls

Also called CUE controls, these controls are a critical component of any SOC Report, as they illustrate to the intended user that the organization has certain roles, responsibilities and obligations in helping the service organization achieve the control objectives stated in the description of the system.

This means that your organization is responsible for reviewing and implementing all applicable controls. Ultimately, your organization plays an active part in supporting the operating effectiveness of your vendor. Without implementing the Complimentary User Entity (CUE) Controls, the service organization’s controls will not operate as intended, thus potentially producing material weaknesses.

Complementary user entity controls (CUECs) are processes you, the consumer of the service or product, need to perform, or have in place to ensure the vendor’s controls operate as expected. A common CUEC would be one that relates to account management. If the vendor provides a web portal that your employees log into, an associated CUEC would be access management. This is because the vendor won’t know when an employee should no longer have access to the portal, so a process or control on your side would need to be in place to notify the vendor of user access terminations. Your control complements the vendors.

CUECs should be reviewed and fully understood as you will want to document:

* Whether they apply to you
* What role or team is responsible for each control
* Whether the control is already addressed by your existing controls
* What controls are not yet in place